TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program

September 1, 2015

Reference Number: 2015-20-079

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
3 = Other Identifying Information of an Individual or Individuals

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

STRONGER ACCESS CONTROLS AND FURTHER SYSTEM ENHANCEMENTS ARE NEEDED TO EFFECTIVELY SUPPORT THE PRIVACY IMPACT ASSESSMENT PROGRAM

Highlights

Final Report issued on September 1, 2015

Highlights of Reference Number: 2015-20-079 to the Internal Revenue Service Director, Privacy, Governmental Liaison, and Disclosure.

IMPACT ON TAXPAYERS

A Privacy and Civil Liberties Impact Assessment (PCLIA) is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form, such as Social Security Numbers, about members of the public and agency employees. Among the most basic of taxpayers' and employees' rights is an expectation that the IRS will protect the confidentiality of personal, financial, and employment information.

WHY TIGTA DID THE AUDIT

This audit was initiated because the Consolidated Appropriations Act of 2005, Section 522, requires the Inspector General to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures every two years. The overall objective of this review was to determine whether the Privacy Impact Assessment Management System (PIAMS) is effectively working as intended to support the privacy impact assessment program and is secure against unauthorized access.

WHAT TIGTA FOUND

The Privacy, Governmental Liaison, and Disclosure (PGLD) organization's Privacy Compliance and Assurance office has responsibility for oversight of the PCLIA process. To comply with applicable laws and regulations governing privacy, the IRS requires system owners to submit all new PCLIAs through the PIAMS. The PGLD organization fully implemented five of the nine recommendations made to address the weaknesses reported in the Fiscal Year 2013 review and implemented suggested user modifications to the PIAMS to effectively support the IRS's privacy impact assessment program. However, PIAMS access control improvements and additional system enhancements are needed. During our audit, TIGTA determined that the Privacy Compliance and Assurance office was unable to provide authorizations supporting access to the PIAMS for 27 of 29 users with elevated privileges and changed the user roles and account statuses for 10 of the 29 users on the PIAMS. In addition, after TIGTA brought it to the PGLD organization's attention, it removed 12 of 41 users' accesses to its shared drive because they no longer had a business need.

During our independent testing, which included creating a fictitious PCLIA in a simulated process, TIGTA identified enhancements that could improve the assessment process. The enhancements included requiring a negative response when no sensitive information is identified in the PCLIA prior to the disclosure review for redaction.

WHAT TIGTA RECOMMENDED

TIGTA made six recommendations, including that the Director, PGLD, issue a communication to PGLD organization managers and employees reminding them to review user accounts for compliance with account management requirements and change the planned corrective action status from closed to open for corrective actions TIGTA identified as not fully implemented.

IRS management agreed with four of our six recommendations. The IRS disagreed with requiring system owners to provide a negative response when they review the assessment for sensitive information and with reopening planned corrective actions that were not fully implemented. TIGTA believes the negative responses are needed to provide assurance that requirements were received and understood, and that prematurely closed corrective actions should be reopened until fully completed to be consistent with Federal requirements.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 1, 2015

MEMORANDUM FOR DIRECTOR, PRIVACY, GOVERNMENTAL LIAISON, AND DISCLOSURE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program (Audit #201520002)

This report presents the results of our review of the Internal Revenue Service's Privacy Impact Assessment Management System. The overall objective of this review was to determine whether the Privacy Impact Assessment Management System is effectively working as intended to support the privacy impact assessment program and is secure against unauthorized access. The Consolidated Appropriations Act of 2005, Section 522,[1] requires the Inspector General to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures every two years. This audit is a mandatory review that is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. 108-447, 188 Stat. 2813, 5 U.S.C. 522a.

Table of Contents

Abbreviations

IRS	Internal Revenue Service
PCA	Privacy Compliance and Assurance
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison, and Disclosure
PIA	Privacy Impact Assessment
PIAMS	Privacy Impact Assessment Management System
TIGTA	Treasury Inspector General for Tax Administration

Background

Within the Federal Government, privacy is defined as an individual's expectation that his or her personal information collected for official Government business will be protected from unauthorized use and access. Privacy is governed by several laws, including the following:

- The Privacy Act of 1974[1] regulates what personal information the Federal Government can collect about private individuals and how that information can be used.
- The E-Government Act of 2002[2] provides additional protection for personal information by requiring agencies to conduct Privacy Impact Assessments (PIA).
- The Consolidated Appropriations Act of 2005, Section 522,[3] requires each agency to establish a Chief Privacy Officer who assumes the responsibility for privacy and data protection policy. This legislation also requires the Inspector General to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures every two years.

The vehicle for addressing privacy issues is the PIA. A PIA is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form, such as Social Security Numbers, about members of the public and, per Internal Revenue Service (IRS) policy, agency employees. In addition, the PIA identifies and is used to evaluate protections to mitigate the impact to privacy of collecting such information. Thus, the PIA is a set of questions that help define how a system affects taxpayers' or employees' privacy and provides a means to assure compliance with applicable laws and regulations governing privacy. A PIA is required to be performed and updated every three years or when a major system change creates new privacy risks. In November 2013, the Department of the Treasury issued guidance that expanded the scope of the PIAs to include questions on civil liberties. As a result, most PIAs are now referred to as the Privacy and Civil Liberties Impact Assessment (PCLIA).[4] The name of the assessment changed to reflect the expanded duties of the Department of the Treasury's Assistant Secretary for Management.

The IRS has the responsibility for ensuring the privacy, confidentiality, integrity, and availability of taxpayer and employee information. Among the most basic of taxpayers' and employees' rights is an expectation that the IRS will protect the confidentiality of personal, financial, and

[1] 5 U.S.C. § 552a (a)(5).
[2] Pub. L. No. 107-347, 116 Stat. 2899, sec. 208.
[3] Pub. L. No. 108-447, 118 Stat. 2813, 5 U.S.C. § 522a.
[4] The IRS uses the term PCLIA only for the PIAs residing on the Privacy Impact Assessment Management System. For surveys, SharePoint sites, and social media and third-party websites not in the PIAMS, the assessments are still known as the PIAs.

employment information. Taxpayers and employees also have the right to expect that the IRS will collect, maintain, use, and disseminate Personally Identifiable Information and data only as authorized by law and as necessary to carry out agency responsibilities. Within the IRS, the Privacy, Governmental Liaison, and Disclosure (PGLD) organization has overall responsibility for privacy issues. The Privacy Policy and Compliance office, within the PGLD organization, promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions. The specific group responsible for oversight of the PIA process is the Privacy Compliance and Assurance (PCA) office.

The IRS takes the protection of taxpayer privacy very seriously. For example, during Calendar Year 2014, the IRS sent 20,947 letters to taxpayers informing them that their personal information was potentially disclosed, costing the IRS more than $149,000 in redeemed credit monitoring services. One single incident accounted for 18,782 of the letters sent to taxpayers and cost the IRS more than $139,000. More recently in May 2015, one of IRS's online applications, Get Transcript,[5] was exploited and unauthorized attempts to access information were made on approximately 204,000 taxpayer accounts. The IRS sent letters to approximately 104,000 taxpayers whose accounts and personal information were compromised and offered them credit monitoring services. The IRS plans to notify the remaining 100,000 taxpayers that third parties appear to have gained access to their personal information from outside the IRS. As of June 2015, the IRS is continuing its investigation and calculating the cost of the incident.

To comply with applicable laws and regulations governing privacy, the IRS requires system owners to submit all new PCLIAs through the Privacy Impact Assessment Management System (PIAMS). The PIAMS is a series of web pages that allow IRS employees to input required PCLIAs online.[6] It provides the PCA office with an automated system to track the PCLIAs and provides its analysts with the capability to perform quality reviews of the assessments. In February 2013, the Treasury Inspector General for Tax Administration (TIGTA) reported[7] that the IRS had not established an effective process to ensure that a PCLIA[8] was completed for all required information technology systems and collections of information that store or process Personally Identifiable Information. Specifically, the IRS did not:

- Establish an effective process to ensure that a PCLIA was completed for all required computer systems that store or process Personally Identifiable Information.

[5] Get Transcript is an online service that allows taxpayers the ability to download transcripts of their accounts for the current and prior three tax years for a tax return, record of account, and verification of nonfiling transcript. The application also provides the current and prior nine tax years for a tax account and wage and income transcript.
[6] During the audit, we determined that the PIAMS contains employee Personally Identifiable Information as it relates to the system owner and others involved with the submission of the PCLIA.
[7] TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* (Feb. 2013).
[8] The term PCLIA is used hereafter for weaknesses that address the PIAs as reported in the February 2013 review for consistency except when surveys, SharePoint sites, and social media and third-party websites are discussed.

- Update the PCLIAs every three years as required.
- Establish an effective process to ensure that the PIAs were completed for customer surveys when necessary. Customer surveys are an important and useful tool for the IRS to measure program effectiveness, customer satisfaction, and delivery of services, but care must be taken to collect, use, disclose, or share Personally Identifiable Information during the survey process.
- Have an effective process to ensure that the PCLIAs for systems containing taxpayer information are posted to its public website. The Office of Management and Budget directs agencies, when practicable, to make the PCLIA publicly available through its website, when information systems and collections of information containing taxpayer Personally Identifiable Information require a PCLIA.
- Complete the PIAs for its SharePoint sites and did not provide correct guidance in the Internal Revenue Manual that SharePoint sites should require the PIAs.
- Establish an effective process to ensure compliance with the Office of Management and Budget's third-party website requirement and to ensure that its privacy notice and a link to its privacy policy were posted on public websites used by IRS officials.
- Ensure that complete and up-to-date written guidelines were prepared for analysts who perform assessments and reviews, and process the PIAs.

In addition, the review component of the PCLIA process in the PIAMS was not effectively automated. It was not effectively tested by the system owners or the analysts who perform quality reviews of the assessments. TIGTA made 11 recommendations to address the reported weaknesses. The IRS agreed with nine and responded that it took action on the remaining two prior to TIGTA making the recommendations. TIGTA included the two recommendations in the report because the evidence was either not present or not sufficient prior to issuing the report.

This review was performed at the PGLD organization's PCA office in the IRS's Headquarters Office in Washington, D.C., and its office in Philadelphia, Pennsylvania, during the period January through June 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The PGLD organization fully implemented five of the nine recommendations made to address the weaknesses reported in the Fiscal Year 2013 review and implemented suggested user modifications to the PIAMS to effectively support the IRS's PIAMS goals and PIA program. In addition, we followed up on the two recommendations for which the IRS responded that it took action prior to TIGTA making the recommendations and determined that they were fully implemented. Specifically, the PGLD organization:

- Documented the new PIA customer survey processes on the organizational website.
- Updated the PIAMS functionality to automatically notify the PCA office and the IRS public website web master when actions are required to process new or existing PCLIAs for public posting.
- Completed and published a new SharePoint PIA template on the organizational website and issued a memorandum advising all business operating divisions of the new template.
- Issued a memorandum to all IRS executives, in conjunction with the Communication and Liaison Division, requesting that the New Media Governance Council[9] be notified of any proposed third-party website activity so it can be reviewed and approved by the Council.
- Implemented a process in which the IRS continuously monitors the Internet for unauthorized third-party websites, coordinated with website owners to ensure that the IRS privacy notice is posted, and provided a link to the IRS's policy on privacy. In Calendar Year 2014, the social media working group in support of the Council identified three Facebook and two Twitter sites using the official IRS logo. The working group reported the sites to the IRS's Office of Online Fraud Detection and Prevention[10] and the sites were removed.
- Provided documented support, and an analyst involved in the PCLIA process confirmed, that the PCLIA template was rewritten and rearranged into an effective, comprehensive electronic assessment of privacy risks. In addition, the PGLD organization reprioritized several updates to the PIAMS based on customer feedback and its own evaluations.

[9] The Council serves as an advisory body for oversight, coordination, and providing input and guidance on major decisions related to the development and implementation of new media channels.
[10] The Office of Online Fraud Detection and Prevention was created to address the increasing and evolving threat of online fraud affecting the IRS and taxpayers. The mission is to reduce online fraud against the IRS and taxpayers.

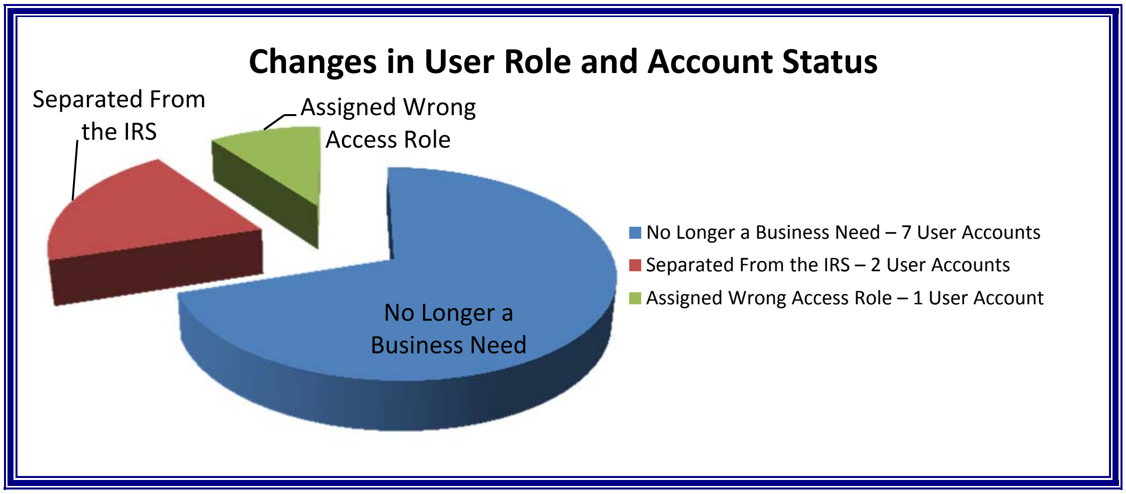
Despite these accomplishments, PIAMS access control improvements and additional system enhancements are needed. In addition, the PCA office needs to continue its efforts to fully implement the remaining four recommendations.

Employees Had Access to the Privacy Impact Assessment Management System Without Documented Authorizations and a Continued Business Need to Know

The PCA office did not use the Service-wide process, the Online 5081 system, to register and grant users access to the PIAMS. Rather, PCA office officials stated that they granted access to users requesting elevated privileges[11] on the PIAMS via e-mail, during meetings, and through telephone approvals from management. The Associate Director, PCA, and PIAMS Administrator determined whether there was a business need and whether access should be granted. The PCA office provided a system report identifying users with elevated privileges, but it was unable to provide any authorizations supporting the access to the PIAMS for 27 (93 percent) of 29 users. After we inquired about the access controls over users with elevated privileges, PCA office officials changed the user roles and account statuses for 10 (34 percent) of the 29 users. For example, at the time of our review, PCA office officials changed the access role of a user who no longer had a business need from "PIAMS Analyst" to "Read Only" access and the user's account status from "Is Active" as "True" to "False." Despite the change in status, the account remained active and the user continued having read-only access to all PCLIAs on the PIAMS because the system did not offer an option to disable the account. As a workaround and to minimize risks, PCA office officials changed the access role to prevent the user from making future edits to any PCLIAs. Figure 1 presents the basis for changes in user role and account status.

[11] PIAMS user accounts with elevated privilege provide access beyond basic PCLIA input and approval from the subject matter expert, program manager, and system owner responsible for answering the assessment questions outside of the PCA office.

Figure 1: Basis for Changes in User Role and Account Status on the PIAMS



Source: TIGTA's analysis of the PIAMS report.

After TIGTA brought to the PCA office's attention that users with elevated privileges should be registered on the Online 5081 system and accounts should be disabled when there is no longer a business need, officials began registering users and working with the contractor to add an option to disable user accounts. The PCA office now requires all users requesting elevated privileges to register on the Online 5081 system prior to granting access to the PIAMS. In addition, in late March 2015, the contractor for the PIAMS added a new feature to disable user accounts.

Besides having access to the PIAMS, PCA office employees, including analysts, also have access to a shared drive that maintains additional PIAs (SharePoint, social media and third-party websites, surveys, and historic PIAs) and other documents related to the PGLD organization. Of 41 users with access to the shared drive, PCA office officials removed 12 (29 percent) users' accesses because the users no longer had a business need and were working outside of the PGLD organization. For example,**********************3************************
*********************************3**
*********************************3**
******3******** These removals occurred after we inquired about access controls.

In addition, a system account, which is no longer being used, existed on the PIAMS. This account was assigned ***************************3**************************
*************************************3************************************
****3********** PCA office officials deleted this account from the system after our inquiry.

The IRS has specific guidance for information technology security. Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance*, requires that the Online 5081 system be used to register all users for access to any IRS information technology resource and that the user be identified, documented, and authorized by the user's manager. In addition, the

manual requires a signed acknowledgment that the user has read, understands, and agrees to abide by the rules of behavior before authorizing access to information and the information systems. These rules of behavior must be reviewed and updated annually at a minimum.

Also, the Internal Revenue Manual provides that Personally Identifiable Information be released to only those individuals having a need to know the information in the performance of their duties. The security principle of least privilege, which allows for only authorized accesses that are necessary to accomplish assigned tasks, be implemented for managing access to shared network drives. Further, accounts should also be reviewed for compliance with requirements at a minimum annually for user accounts and semiannually for elevated privilege accounts. Account managers should be notified when accounts, including system accounts, are no longer needed so that the accounts can be disabled or deleted.

Notwithstanding these established requirements, we identified several factors contributing to the identified weaknesses.

- The current PCA office staff stated that the PIAMS is a tool used to replace the old manual paper PIA process. They further shared that they were not part of the PIAMS implementation team and could not identify in the system development artifacts the reason the Online 5081 system was not used to register and authorize users' access to the PIAMS.
- PCA office officials stated that they conduct informal reviews, which are not documented, of users on the PIAMS to determine if there is a continued business need for access. However, they further stated that their last review of user accounts resulted from our inquiry and request for PIAMS user account information.
- The shared drive coordinator was not aware of the need or given guidelines to review users' accesses for continued business need prior to our audit.
- Because of system limitations created as a result of management not incorporating a disabling feature, management was not capable of disabling a user's account for the PIAMS.

Without registering users on the Online 5081 system, the PCA office and the IRS did not have a central location to identify and account for all system accesses when a user's account is no longer required, when the user transfers or leaves the IRS, or when individual information system usage or need to know changes. As a result, unneeded system accesses may be missed and not removed, users will have continued access to Personally Identifiable Information when there is no longer a need to know, and the access could create potential security vulnerabilities associated with unused active accounts. Also, having an unused system account violates IRS polices and magnifies potential security vulnerabilities when the account provides administrative capabilities.

Lastly, users with elevated privileges on the PIAMS could not use the IRS's standard process (through the Online 5081 system) to acknowledge the IRS system security rules. Moreover, users and their managers could not use the same standard process to annually recertify that the users have a continued business need for access to the PIAMS. Once users are registered on the Online 5081 system, acknowledgement of the security rules is included as part of the application request and approval process, and annual recertifications of continued business need are required. When employees do not acknowledge their responsibilities and expected behavior with regard to information and information system usage, the IRS may experience difficulties in taking disciplinary action when violations of information system usage occur.

Recommendation

Recommendation 1: The Director, PGLD, should issue a communication to PGLD organization managers and employees reminding them to review user accounts on information technology resources that they manage, such as the PIAMS and shared drives, for compliance with account management requirements. These reviews should, at a minimum, be conducted annually and semiannually for elevated privilege accounts.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS planned to issue a communication on August 13, 2015, reminding all PGLD organization system administrators of the requirements to review accesses in accordance with Internal Revenue Manual 10.8.1.

The Privacy Impact Assessment Management System Is Operating As Intended, but Enhancements Can Be Made

As mentioned previously, the IRS requires system owners to submit all new PCLIAs through the PIAMS. Typically, this process is delegated to a subject matter expert, who initiates and completes the assessment online. A checkmark on the PIAMS side menu will indicate when a topic section of the PCLIA is completed. Once the assessment is completed, the subject matter expert uses the PIAMS to generate an e-mail to the system of records notice and records retention analysts that the PCLIA is ready for their review. The analysts review their respective sections and either return the PCLIA for correction or complete their review allowing the subject matter expert to proceed with management's review of the assessment.

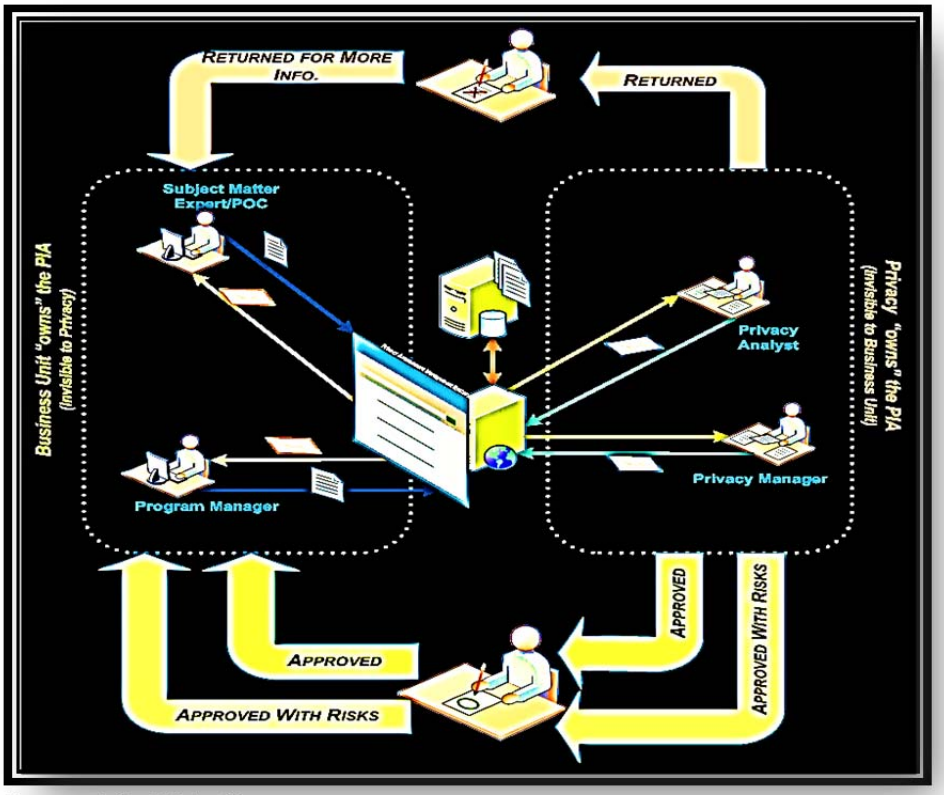
Next, the subject matter expert sends another system-generated e-mail to the program manager (hereafter referred to as the manager) that the assessment is ready for review. If the manager finds that information is missing or certain questions need clarification, the assessment can be returned to the subject matter expert for resolution or the manager can approve the assessment. Management approval generates a PIAMS e-mail to the PCA office that the PCLIA is ready for its review. An analyst is assigned to review the PCLIA and has the option to either accept the assessment or return it to the subject matter expert to clarify questions or to supply missing

documentation. When the issues are addressed, if any, the assessment is resubmitted to the PCA office. Once the analyst accepts the PCLIA, the following types of approvals (and follow-up actions) can be recommended:

- Approved – No Risk: there are no unresolved issues associated with the system PCLIA.
  - Post the PCLIA to the IRS public website.
  - Do not post the PCLIA to the IRS public website.
- Approved – With Risks: there are unresolved issues such as a missing records retention schedule or PCLIA information on associated IRS systems.
  - Post the PCLIA to the IRS public website.
  - Do not post the PCLIA to the IRS public website.

Subsequently, the analyst sends the PCLIA to the Privacy manager for final review, approval, and signature. After signing the assessment, the PIAMS sends another system-generated e-mail to the subject matter expert, manager, and system owner notifying them that the PCLIA has been approved and a copy of the approval memorandum can be accessed through the system. The approval memorandum refers to the E-Government Act, which requires the IRS to make the PCLIA available to the public and requests that the system owner review the assessment to identify any information that would cause harm to the IRS or any party if disclosed. At this time, the PCLIA becomes read-only access and no other modifications can be made. Figure 2 displays the PCLIA process using the PIAMS.

Figure 2: The PCLIA Process in the PIAMS



Source: The PCA office.

The PIAMS is properly sending system-generated e-mails to affected subject matter experts, managers, system owners, and analysts involved with the PCLIA process and is meeting business system requirements. However, during our independent testing, which included creating a fictitious PCLIA in a simulated process, our audit team identified enhancements that could improve the assessment process. These enhancements include:

- The PIAMS e-mail that is sent to the manager should also include the analyst's message requesting clarification or additional information along with the associated assessment question number. This information is provided in the e-mail sent to the subject matter expert, who typically completes the PCLIA, but not to the manager. The manager is notified only that a question within the PCLIA needs clarification; the notification does not specify the text or the assessment question number for reference.
- When clarification or additional information is requested and changes are made to the PCLIA, the PIAMS should route the assessment back to the manager for review and approval. Currently, once the subject matter expert addresses the comments, the PCLIA is sent back to the analyst for review and is then forwarded to the Privacy manager for final review and approval. The manager is not informed or aware of the changes, if any.

- When the Privacy manager approves the PCLIA, the instructions sent to the system owner in the PIAMS e-mail should be clearer and require a response from the system owner as to whether sensitive information is identified for redaction. Specifically, the e-mail should inform the system owner that actions are required, *e.g.*, review and respond, and that he or she needs to access the approval memorandum, which instructs the system owner to review the PCLIA for disclosure and to respond within 10 days if sensitive information is identified. At present, the e-mail informs the system owner only that the PCLIA was approved by the Associate Director, PCA, and that the approval memorandum can be accessed in the PIAMS. The e-mail does not inform the system owner that actions are required or to access the memorandum. Also, current PCA office procedures require a positive response only if sensitive information is identified. However, this process does not provide assurance that the system owner received and understood the requirements; requiring a negative response would provide such assurance.

  To measure the extent and impact of the current limitation, we selected a judgmental sample[12] of 27 IRS information technology systems and e-mailed a questionnaire to 21 individuals listed in the PCLIAs as the system owners[13] to determine whether they received an e-mail notifying them that the PCLIA had been approved and for them to review the assessment for disclosure. Twelve (57 percent) of the 21 system owners responded that they did not receive the e-mail. Four of the 12 employees did not realize they were the owners of the system. The reasons they offered included the employee believed someone else to be the owner or the employee was in an acting management role. Also, **********3********** **********3**********.

  **********3********** **********3********** **********3**********. Otherwise, the PCA office is exposed to the risk of sensitive information being posted to the public website that could cause harm to the IRS. Fortunately, none of the system owners identified any additional sensitive information in the PCLIAs that should have been redacted.

- The side menu on the PCLIA section of the PIAMS should also include the question number associated with each topic to help direct the user to the appropriate section when addressing specific questions. Currently, the menu provides only the topic section, for example, *Section C., Privacy Act & System of Records.* The menu should also inform the user that the section is in reference to question 9 in the PCLIA.

[12] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[13] Four individuals were listed as owners of more than one system.

The Government Accountability Office's *Standards for Internal Control in the Federal Government*[14] provides that control activities, such as managerial approvals, occur at various levels for an entity. The PIAMS should facilitate a more efficient method of completing the PCLIA because it replaces the manual paper-based process. The PCA office stated that these enhancements were not identified as concerns during its PIAMS usability testing and that the current procedures have always been in place for managing and processing the PCLIAs. We are concerned that without proper approvals, managers may not be aware and may not approve changes made to the assessment after their initial review. Also, additional IRS and PCA office resources may be spent to clarify questions or requests for information from the subject matter experts, managers, and system owners involved in the PCLIA process. Further, without a positive or negative response, there is no assurance that system owners received and understood the requirement and action required of them as supported by our test results.

The PCA office met with the contractor to assess the viability of these enhancements and will implement all except requiring a negative response from the system owner. The PCA office will rank the accepted enhancements in priority along with other system modifications in the next PIAMS upgrade, and changes will be made based upon the availability of funds.

Recommendations

The Director, PGLD, should:

Recommendation 2: Require a negative response from the system owner regarding the review of the assessment for sensitive information.

> ***Management's Response:*** The IRS disagreed with this recommendation. The IRS does not believe that requiring a negative response and the associated tracking would be a good use of its limited resources. Instead, the IRS revised the communique to the system owners and outlined the actions required to review and redact sensitive information from the approved PCLIA.
>
> ***Office of Audit Comment:*** The revision does not provide assurance that the system owner received and understood the requirements, which we identified in our audit results. Requiring a negative response would provide such assurance. Otherwise, the PCA office is exposed to the risk of sensitive information being posted to the public website that could cause harm to the IRS.

[14] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

Recommendation 3: Continue to assess, identify, and implement enhancements to improve the functionality of the PIAMS.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to add language to the PGLD organization's five-year plan for PIAMS development requiring the assessment and improvement process to continue as a normal course of business.

Recommendation 4: Provide training, when needed, to stakeholders involved in the PIA process to ensure that no sensitive information is included and documented in the assessments.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to expand guidance it provides to stakeholders via the PGLD organization's intranet site to include training modules for specific stakeholders, such as project managers. The IRS expects the first of four anticipated modules to be available for self-directed online training in the early fall of 2015.

Corrective Actions Were Shown As Completed That Were Not Fully Implemented

We reviewed the Joint Audit Management Enterprise System[15] for the IRS's responses, documentation, and the statuses of the planned corrective actions for the nine agreed recommendations reported in the February 2013 report. All nine of the recommendations were shown as closed as of July 14, 2014, indicating that the corrective actions have been completed. However, we determined that the PGLD organization[16] did not fully implement four of the nine recommendations made to address the reported weaknesses. Specifically, the PGLD organization did not:

- Properly address two parts of a three-part recommendation. The PGLD organization completed planned revisions to the Major Change Determination template to help facilitate the reconciliation process as well as established a reconciliation process for the PCLIA inventory with all the information systems in the IRS As-Built Architecture[17] inventory. However, it did not account for all new systems added to the current

[15] The Department of the Treasury implemented the Joint Audit Management Enterprise System for use by all bureaus to track, monitor, and report the status of internal control audit results. This system tracks specific information on issues, findings, recommendations, and planned corrective actions from audit reports issued by oversight agencies such as TIGTA.

[16] This section of the report will document the responses and corrective actions taken from the PGLD organization's perspective since the February 2013 report recommendations were made to the Director, PGLD.

[17] The IRS As-Built Architecture presents an enterprise view of the IRS's information technology and business environments. It is an integral part of the IRS's enterprise architecture dedicated to documenting the current production environment and related organizations, locations, and technology platforms. It also provides information on whether the system collects Personally Identifiable Information and requires a PCLIA.

production environment. The PGLD organization worked extensively with stakeholders involved with the enterprise life cycle and the As-Built Architecture to establish a reconciliation process. It implemented controls, such as representation at milestones and reauthorization reviews, to ensure that projects have an approved PCLIA and are reflected on the As-Built Architecture. To further assist the reconciliation process, the PGLD organization recommended changes to the As-Built Architecture regarding how PIA information is displayed and linking subsystems to master systems with prevailing PCLIAs. The PGLD organization used the system inventory list[18] from the Fiscal Year 2013 review and updated it using the As-Built Architecture's November 2012 inventory report.

We obtained the As-Built Architecture's monthly reports from April 2012 to April 2015 and identified 36 new systems that were added to the IRS's current production environment. As indicated on the As-Built Architecture, 17 of these systems required a PCLIA. Our analysis determined that three (18 percent) of those systems did not have a PCLIA. These three systems were reported as new systems dating back as early as June 2012. PCA office personnel stated that two of these systems were pre-reconciliation and post inventory report, which resulted in not identifying the systems. For the remaining system, they merely missed it due to the extensive reconciliation process.

While the PGLD organization did establish a process to identify the PCLIAs that had not been updated within three years, it has not coordinated with all system owners to review and update these PCLIAs as required. The PGLD organization reviewed a legacy list with more than 700 PCLIAs or Major Change Determinations that were more than three years old and identified 132 systems that were not updated. For each of these systems, PGLD personnel reached out to and coordinated extensively with the system owners, points of contact, and business unit security program management officers to ensure identification of an updated assessment for those still operating with Personally Identifiable Information. Also, the PGLD organization built an automatic feature in the PIAMS and developed a manual process for the PIAs not yet in the PIAMS to identify assessments not updated within three years.

Our analysis determined that 23 (17 percent) of the 132 PIAs from the legacy list had not been updated within three years and had expired. We were unable to validate the assessment statuses for three of the 132 PIAs. We referred these assessments to the PCA office for follow-up. The PCLIAs for the remaining 106 systems were current assessments, surveys, SharePoint sites, or social media and third-party websites that were not required to be updated. In addition, we reviewed an April 2015 list of the PCLIAs, and our analysis determined that 16 (4 percent) of 385 PCLIAs in the PIAMS were expired. In May 2015, we reviewed 47 (23 percent) of 205 PCLIAs on the IRS public website, and they were expired as well. Further analysis revealed that a more current

[18] This inventory list was dated March 30, 2012.

copy of the PCLIA was available in the PIAMS for 39 of the 47 assessments but was not yet posted. Moreover, 13 of the 205 PCLIAs posted to the website did not have a required approval date.

- Obtain the PCLIAs from system owners for all 184 systems identified as potentially requiring an assessment. The PGLD organization provided in its closing corrective action that personnel had conducted in-depth investigations into these systems to determine whether they required a PCLIA. It worked with stakeholders across every business unit and within the Information Technology organizations and narrowed the list to 100 systems for the system owners to provide assessments.

  Our review determined that 114 of the 184 systems require an assessment as indicated on the As-Built Architecture. The difference between the PCA office's and our analyses is the net amount from the PCA office's initial analysis and current information on the As-Built Architecture of whether systems require the PCLIAs due to factors such as systems no longer in operation and reassessments of whether a PCLIA is required. We also determined that the PGLD organization did not obtain the PCLIAs for two (2 percent) of the 114 systems. PCA office personnel did not identify these systems, but they are working to secure new PCLIAs.

- Ensure that the 80 PCLIAs identified as not posted to the IRS public website were redacted and made available to the public, where applicable. The PGLD organization conducted an analysis and determined that several PCLIAs did not require posting to the public website for various reasons, such as assessments that were initially prepared were not completed and some documents were not assessments but rather were qualifying questionnaires used in determining whether a PCLIA was necessary. As a result of its analysis, PGLD organization personnel posted 25 PCLIAs to the IRS's website.

  Our analysis of the As-Built Architecture determined that 58 of the 80 PCLIAs were for systems no longer in operation or did not require a PCLIA. Therefore, they were not required to be posted. For the remaining 22 PCLIAs, 20 were posted. The difference between the PCA office's and our analyses is due to systems that are no longer in operation. However, we also determined that the PGLD organization did not post a current PCLIA for two (9 percent) of the 22 systems to the public website. The PCLIAs for these two systems had expired and were deleted from the website. PCA office management stated that it is their policy to delete the PCLIAs when expired rather than replace them upon receipt of a current assessment. However, the PCA office never received a current PCLIA from the system owners. PCA office management stated that they are also aware of the need to update the IRS public website with current PCLIAs and have reassigned this task to another analyst after four employees who previously had the task were reassigned.

- Ensure that current and complete standard operating procedures were established for all PIA processing procedures, including updating, reviewing, approving, and reconciling

the PIAs to other IRS system inventories. In February 2014, the PGLD organization provided in its closing corrective action that it had completed the standard operating procedures for all PIA processing as recommended and will incorporate these procedures into a new Internal Revenue Manual section (10.5.2, *Privacy Compliance*) that is under development.

Our review determined that the PGLD organization prepared eight documents for these procedures. However, five of these documents have not been finalized and are not incorporated in the new Internal Revenue Manual. PCA office personnel stated that these standard operating procedures were completed and are being used but that they neglected to sign them. We secured the missing signatures for the five documents prior to issuing this report.

The IRS has specific guidance over the closure of weaknesses reported for its internal control program. Internal Revenue Manual 1.4.30, *Monitoring Internal Control Planned Corrective Actions*, requires that recommendations are appropriate and implemented, corrective actions are taken in a timely fashion through independent verification, and validations occur. In addition, Government Accountability Office guidance provides that management should complete and document corrective actions to remediate internal control deficiencies on a timely basis. The corrective action is completed only after action has been taken that 1) corrects identified deficiencies, 2) produces improvements, or 3) demonstrates that the findings and recommendations do not warrant management action.

Without the proper closing of reported weaknesses, the IRS cannot be assured that its internal control program is operating as intended. As a result, the IRS cannot assure its stakeholders that planned corrective actions were implemented as reported in correcting the weaknesses. In addition, the IRS will not be meeting its legislative requirements to prepare the PCLIAs for systems that collect Personally Identifiable Information.

Recommendations

The Director, PGLD, should:

Recommendation 5: Notify the Associate Chief Financial Officer for Corporate Planning and Internal Control's office to change the planned corrective action status from closed to open on the Joint Audit Management Enterprise System for the corrective actions that TIGTA identified as not fully implemented. The statuses of these planned corrective actions should be reopened until they are fully implemented and fulfill the original audit recommendations as agreed to in TIGTA's Fiscal Year 2013 report.

Management's Response: The IRS disagreed with changing the status of the closed recommendations. IRS management shared that all of the recommended actions from the Fiscal Year 2013 audit report were substantially completed and met the intent of the

recommendations. IRS management plans to secure the small number of items identified during the audit and will notify the audit team once they are completed.

Office of Audit Comment: We believe that planned corrective actions should remain open until they are fully completed. Closing planned corrective actions prematurely is not consistent with Federal requirements and increases the risk that deficiencies we previously identified will still exist, as was evidenced in this report.

Recommendation 6: Revise current policy to reflect that expired PCLIAs on the IRS public website should not be deleted but instead should be replaced upon receipt of current assessments.

Management's Response: The IRS agreed with this recommendation. The PGLD organization plans for its current processes to reflect the intent of the recommendation. To document the procedures, the PGLD organization plans to update the Redaction and Posting Standard Operating Procedure to state that expired PCLIAs will not be deleted until they are replaced by an updated PCLIA.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the PIAMS is effectively working as intended to support the PIA program and is secure against unauthorized access. To accomplish our objective, we:

I. Determined whether the planned corrective actions for recommendations from the February 2013 report[1] enhanced the effectiveness of the PIA process.

- A. Obtained background information and requirements for privacy and the PIA program.
- B. Determined whether the previously reported weaknesses and planned corrective actions from the February 2013 report were fully implemented, validated, and properly closed.
- C. Simulated the PCLIA process to determine whether the PIAMS is operating as intended.
- D. Obtained the results from Steps I.B. and I.C. and assessed whether the planned corrective actions taken support achieving the intent and goals of the PIAMS.
- E. Determined the causes for the conditions reported.

II. Determined the effectiveness of computer security and access controls for users, which includes users with elevated privileges, on the PIAMS and to the PGLD organization's shared drive that contains the PIAs.

- A. Reviewed Internal Revenue Manual 10.8.1, *Information Technology Security*, and any other policies to identify procedures and guidelines when granting users access to IRS computer systems.
- B. Determined the process for approving and granting users elevated privilege access on the PIAMS and access to the shared drive that contains the PIAs.
- C. To assess access controls, used audit team members as the subject matter expert, manager, and system owner responsible for answering the assessment questions. We requested another TIGTA auditor to attempt access to the fictitious assessment created in Step I.C. to determine whether access to the PCLIA is limited to only those who were granted permission.

[1] TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* (Feb. 2013).

D. Determined whether elevated privilege user accounts for shared, generic, duplicate, or default accounts exist.

E. Determined whether elevated privilege user accounts not accessed within 120 calendar days exist by reviewing the last login to the PIAMS. We determined whether the accounts are regularly reviewed to identify inactive accounts and whether accounts are no longer needed.

F. Determined whether elevated privilege user accounts for separated employees exist by comparing all users to the Treasury Integrated Management Information System[2] for the current pay period. If users were not identified, we searched the Treasury Integrated Management Information System's separated employees list to determine when the employees separated.

G. Determined whether elevated privilege user accounts activities are regularly reviewed independently for suspicious activities, computer configuration changes, and other potential security issues.

H. Determined whether the PIAMS completed a security assessment. We selected a judgmental sample[3] of 27 of 441 PCLIAs from the PIAMS to determine whether the system contains sensitive information, which is the basis in assessing whether a security assessment would be conducted. We used a judgmental sample because we wanted to select the PCLIA with the highest probability of containing sensitive information.

I. Determined the causes for the conditions reported.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Treasury Directives, Office of Management and Budget Memoranda, and the Internal Revenue Manual for evaluating the use of information in identifiable form, privacy and data protection procedures, and computer security controls. We evaluated these internal controls by interviewing Department of the Treasury officials, IRS PGLD organization personnel, and the PCA office team; reviewing enterprise life cycle artifacts; and reviewing documents supporting the closure of weaknesses reported in the February 2013 report.

[2] The Treasury Integrated Management Information System is an official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. It is managed by the Department of the Treasury.
[3] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Louis Lee, Lead Auditor
Cindy Harris, Senior Auditor
Ashley Weaver, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Risk Management Division OS:CTO:SP:RM
Chief Financial Officer OS:CFO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluations and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Chief Financial Officer OS:CFO
    Director, Privacy, Governmental Liaison, and Disclosure OS:P

Appendix IV

Management's Response to the Draft Report

PRIVACY, GOVERNMENTAL LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 14, 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Mary J. Howard
Director, Privacy, Governmental Liaison and Disclosure

SUBJECT: *Draft Audit Report* – Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program (Audit #201520002)

Thank you for the opportunity to respond to the above referenced draft audit report. Ensuring the privacy and security of data is a top priority for the IRS and a fundamental component of maintaining the public trust in the tax system and promoting voluntary compliance.

We are pleased TIGTA acknowledged that the IRS takes the protection of taxpayer privacy very seriously. In fact, the IRS continues to be a model for privacy practices within the federal government and remains at the forefront of government privacy initiatives. In addition to the Privacy Civil Liberties Impact Assessment (PCLIA) (previously known as Privacy Impact Assessment) process reviewed in this audit, the IRS works to improve privacy protections in a number of ways. We partner with the Department of Treasury to implement the latest in civil liberties protections, institute guidance from the National Institute of Standards & Technology, aggressively address instances of data loss or fraud and develop mitigation strategies, and actively review and update privacy policy and training to address emerging concerns. Additionally, we increased the staffing in our Privacy Policy and Compliance operation to proactively address privacy as IRS pursues expanded service for taxpayers by using digital and on-line interactions.

Privacy Impact Assessments took a major step forward with the deployment of the PIA Management System (PIAMS) in December 2011. Since the deployment, we continually made improvements based on feedback from users and those reviewing the PCLIAs. The additional improvements identified by the auditors will be included in prioritized change requests and implemented when funds become available.

The PIAMS system is not a system in the traditional sense. It is a series of web pages that allow for the flow of information between the PIA submitters and Privacy employees. The names of the IRS employees submitting the assessment, as part of the work assignments, are the only personally identifiable information stored on the PIAMS pages and that employee information is readily available to the public. The PIAMS system is not linked to other IRS systems, such as the master file or other systems containing taxpayer information, therefore the risk of unauthorized access is very low. The approval process in place for elevated access is adequate for the type of information contained in PIAMS. We also implemented the OL5081 approval path to further strengthen existing controls.

This audit also reviewed the corrective actions taken in response to the 2013 audit of the PIAMS process. As the PIAMS system and resulting PIA processes were relatively new at the time of the prior audit, there were a number of recommendations. Some of those recommendations required the analysis of a large number of systems used by the IRS to deliver the IRS Mission. We feel that all of the recommendations from the prior audit were substantially implemented. We implemented/completed the following activities:

- Established a reconciliation process between the As Built Architecture and the PCLIA inventory;
- Researched and secured a large number of outstanding PCLIAs;
- Added a trigger in PIAMS to identify PCLIAs as they approach the three year review cycle;
- Established and posted instructions for SharePoint PIAs on the PGLD webpage; and
- Developed Reports for better management control.

While we believe the prior recommendations were fully implemented, we understand that the audit team believed a few items required additional action. We are addressing those issues immediately.

If you have any questions, please contact me at (202) 317-6449, or a member of your staff may contact Frances Kleckley, Director, Privacy Policy and Compliance at (803) 312-7786.

Attachment

Attachment

Draft Audit Report – Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program (Audit #201520002)

RECOMMENDATION 1: The Director, PGLD, should issue a communication to PGLD organization managers and employees reminding them to review user accounts on information technology resources that they manage, such as the PIAMS and shared drives, for compliance with account management requirements. These reviews should, at a minimum, be conducted annually and semiannually for elevated privilege accounts.

CORRECTIVE ACTION: We agree with this recommendation. Ensuring that only those with a business need have access to systems, applications and storage sites is critical to securing sensitive information. The PGLD Director will issue a communication on August 13, 2015 reminding all PGLD system administrators of the requirements to review accesses in accordance with IRM 10.8.1.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 2: Require a negative response from the system owner regarding the review of the assessment for sensitive information.

CORRECTIVE ACTION: We disagree with this recommendation. While we agree with the intent of the recommendation, we do not believe requiring a negative response and the associated tracking of such a process would be a good use of our limited resources. Instead, we revised the communique to system owners and outlined the actions required to review and redact sensitive information from the approved PCLIA. This review is in addition to the review conducted by the PGLD Disclosure to identify any sensitive information prior to posting an approved PCLIA on the public website.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 3: Continue to assess, identify, and implement enhancements to improve the functionality of the PIAMS.

CORRECTIVE ACTION: We agree with this recommendation. As stated earlier in this response, we have continually assessed the PIAMS system and, as funding has allowed, implemented enhancements to improve the functionality since the deployment in December of 2011. We added language to our Five Year plan for PIAMS development requiring this assessment and improvement process continue as a normal course of business.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 4: Provide training, when needed, to stakeholders involved in the PIA process to ensure that no sensitive information is included and documented in the assessments.

CORRECTIVE ACTION: We agree with this recommendation. Since the deployment of PIAMS, we have provided guidance to stakeholders via the PGLD intranet site. We are expanding this guidance to include training modules for specific stakeholders, such as project managers. We expect the first of four anticipated modules to be available for self-directed on-line training in the early fall of 2015.

IMPLEMENTATION DATE: October 15, 2015

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 5: Notify the Associate Chief Financial Officer for Corporate Planning and Internal Control's office to change the planned corrective action status from closed to open on the Joint Audit Management Enterprise System for the corrective actions that TIGTA identified as not fully implemented. The statuses of these planned corrective actions should be reopened until they are fully implemented and fulfill the original audit recommendations as agreed to in TIGTA's Fiscal Year 2013 report.

CORRECTIVE ACTION: We disagree with changing the status of the closed recommendations. All of the recommended actions from the 2013 audit report were substantially completed and met the intent of the recommendations. The small number of items identified during this audit will be secured and we will notify the audit team once that process is completed.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 6: Revise current policy to reflect that expired PCLIAs on the IRS public website should not be deleted but instead should be replaced upon receipt of current assessments.

CORRECTIVE ACTION: We agree with this recommendation. Our current processes now reflect the intent of this recommendation. In order to document the procedures we updated the Redaction and Posting Standard Operating Procedure to state that expired PCLIAs will not be deleted until they are replaced by an updated PCLIA.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: N/A